Security Automation Protocols (SAP) and NIEM User Stories & Wish Lists

Tom Millar, US-CERT

First of all: NIEM?

- NIEM is the National Information Exchange Model
- All agencies are required to evaluate the use of NIEM for information exchange development per OMB’s *Agency Information Sharing Functional Specification* (March 4, 2010)
- Lots on wikipedia, more on niem.gov

NIEM and SAP in harmony

- NIEM could potentially leverage the SAPs by adapting them as an external namespace;
- Or: NIEM’s conformance rules could be leveraged in future SAP developments for maximum interoperability;
- Or a third path – let’s just not break anything that already works!

ITAP: User Stories

- We have to process hundreds of incident reports a day
- We all want to automate as much of the reporting and updating activity as possible
- It would be particularly satisfying if the results could be leveraged in interesting ways (actionable metrics!)

ITAP: What If ?

- …We wrap CEE logfiles in a schema like IODEF?
- Along with MAEC-formatted malware data?
- …We start using CAPEC and CWE references to help find root cause?
- What about a Common Incident Impact Severity Scoring System?

EMAP User Stories

- We have to process millions of system and network events a day
- We constantly have to re-parse text
- We want to tighten up the OODA loop for detection and response
- It would be terrific if we could automatically share anonymized event patterns with our other brains too

EMAP: What If ?

- …We leverage something like FLAIM with CEE for sharing traffic and logs?
- Along with references to MAEC, CAPEC, CWE or CVE in alert messages?
- …We can tie OVAL checks to event patterns to quickly surmise the state of a target?

TAAP User Stories

- We track dozens of threat families a day
- We push dozens of PDFs and write hundreds of lines of custom code to try and help each other out
- We constantly try to keep up with dozens of feeds, blogs, lists, and ad hoc threads across multiple environments
- We help mitigate when there’s time

TAAP: What If ?

- …We could annotate families in MAEC metadata, and document relationships?
- …We could use XCCDF and OVAL to build standard post-compromise mitigation checklists?
- …We could employ a handling standard like TLP across threat reporting elements, for automatic “tearlines?”